

M303

TMA 03

2020J

Mainly covers Book C *Numbers and rings*
Cut-off date 26 January 2021

You will find instructions for completing TMAs in the ‘Assessment’ area of the M303 website. Please remind yourself of these instructions before beginning work on this TMA. You can submit this TMA either by post, together with a completed TMA form (PT3), to arrive by the cut-off date given above, or electronically, as a single PDF file, using the University’s online TMA/EMA service.

Half of the TMA is formative, and the other half is summative. The formative questions are designed to either *extend* your understanding of the topics or *introduce* the topics of later books, while the summative questions place more emphasis on *assessing* your understanding of the topics. Both types of question will be marked by your tutor, but (unlike the summative questions) marks for the formative questions do not count towards your final grade. You should submit your solutions to both sets of questions to your tutor by the cut-off date.

The marks allocated to each part of a question are indicated in the margin.

Although many of the questions on this assignment require numerical answers, the questions invariably carry *method marks*.

In phrasing the questions, we have used the words listed below, each of which should be interpreted as indicated.

prove, show, explain, justify	Clear reasoning and explanation for all steps are called for.
determine, find, devise, calculate, compute	An indication of the method used and all working in arriving at an answer should be given.
deduce	Clear explanation of how one result follows from another is required.
solve	Working must be shown. A numerical answer alone is not sufficient.
evaluate, give, write down, list	Answer suffices. No explanation need be given.
hence	No marks will be awarded for any alternative method.

This TMA is based on Book C (Numbers and rings), except for the formative Question 7, which covers the start of Book D.

Part A is **summative**. These questions assess your knowledge of the module. You must not discuss these questions in the forums, and your tutor is not allowed to help you directly.

Part B is **formative**. You should choose two questions to submit to your tutor for feedback, and we suggest that one of these is Question 7 since this will help you with the next TMA.

Doing the formative questions will help you to understand key concepts covered in the text. You are encouraged to discuss these questions in the module forums and with your tutor (who is allowed to help you).

Question 7 is designed to help you with TMA 04. Questions 8 and 9 cover material that is more central to the module, while Question 10 is designed to expand your understanding beyond the core material.

Your tutor will mark all of the answers that you submit. But note that only your marks for Part A count towards your overall continuous assessment score.

Part A Summative

Question 1 – 8 marks

- (a) Determine the smallest positive integer that has exactly 45 distinct positive divisors, including itself and 1. [4]
- (b) Prove that if p^2 divides n , where p is prime, then

$$\phi(n) = p\phi(n/p),$$

where ϕ is Euler's phi-function. [4]

Question 2 – 10 marks

- (a) Determine whether or not the quadratic congruence

$$5x^2 + 7x + 3 \equiv 0 \pmod{17}$$

has solutions:

- (i) by using Euler's Criterion; [2]
- (ii) by using Gauss's Lemma. [2]
- (b) Using the Law of Quadratic Reciprocity in conjunction with Theorem 2.2 and Proposition 3.2 of Chapter 10, determine the values of the Legendre symbols

$$\left(-8/47\right), \quad \left(227/31\right) \quad \text{and} \quad \left(227/307\right).$$

(Note that each of 31, 47, 227 and 307 is prime.) [6]

Question 3 – 9 marks

Throughout this question, let $f(x) = x^6 - 3x^4 - 4x^3 + 3x + 3$ and $g(x) = x^3 - 3x - 3$.

- (a) Use Eisenstein's Criterion to show that $g(x)$ is irreducible in $\mathbb{Q}[x]$. [1]
- (b) Use the Rational Root Test to find all rational roots of $f(x)$. [4]
- (c) Show that $g(x)$ divides $f(x)$, and hence express $f(x)$ as a product of irreducible polynomials over $\mathbb{Q}$. [4]

Question 4 – 10 marks

- (a) Suppose that $\sqrt{10} = \frac{m}{n}$, where m and n are positive integers. Show that

$$\sqrt{10} = \frac{10n - 3m}{m - 3n},$$

and explain how the method of infinite descent can be used to deduce from this that $\sqrt{10}$ is irrational. [5]

- (b) One of the numbers 1170 and 1197 can be written as the sum of two squares, and the other cannot. Explain why one cannot be so written, and write the other as a sum of two positive squares in *two* different ways. [5]

Question 5 – 10 marks

Let

$$R = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, \text{ hcf}(a, b) = 1, b \text{ is odd} \right\}.$$

That is, R is the set of all rational numbers that, when written in lowest terms, have odd denominator.

- (a) Show that R is a subring of $\mathbb{Q}$, and explain why R is therefore an integral domain. [3]
- (b) What are the units of R ? [2]
- (c) Write $a = 2^r c$ for some $r \geq 0$ and odd integer c . Prove that the element a/b of R is irreducible in R if and only if $r = 1$.
Hint: consider the cases $r = 0$, $r = 1$ and $r > 1$ separately. [3]
- (d) Hence, or otherwise, show that every prime element of R is an associate of the element 2 ($= 2/1$). [2]

Question 6 – 3 marks

For this TMA, we would like you to post something in the Book C forum that is about the mathematics in Book C. To earn full marks, provide either a screenshot of your forum post or directions as to where to find it (giving the thread title, time and date). (If you are not in a position to provide such evidence, contact your tutor for advice.) [3]

Part B Formative

Question 7 – 11 marks

This question concerns Chapter 13 of Book D, and relates to Question 5 in TMA 04.

We define three subsets of the plane (using set notation) as follows:

$$A = \{(x, y) \in \mathbb{R}^2 : 1 < x^2 + y^2 \leq 5\},$$

$$B = \{(x, y) \in \mathbb{R}^2 : y \geq 1\}$$

and

$$C = A \cap B.$$

- (a) Sketch on separate diagrams, by hand or otherwise, the sets A , B and C , taking care to distinguish between points that lie inside and outside the sets. [6]

You should follow the conventions used in the module text by using dashed lines to indicate the boundaries of open sets and solid lines to indicate the boundaries of closed sets. The status of individual points can be indicated by using small circles for excluded points and filled discs for included ones.

- (b) Use Definition 3.4 of Chapter 13 to determine whether the limit of the sequence $\left((0, 1 + \frac{1}{n})\right)_{n=1}^{\infty}$ is in C . [5]

Question 8 – 14 marks

This question gives you practice in working with polynomials. It also gives you a chance to practise use of the $\sum$ notation for summation.

- (a) Let $f(x)$ be a polynomial in $\mathbb{Q}[x]$ with

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n = \sum_{i=0}^n a_i x^i.$$

Write down each of the following products using the summation notation, taking care in your answer to ensure that the summands each contain only a single power of x .

- (i) $x f(x)$
(ii) $(x + 1) f(x)$
(iii) $(b_0 + b_1x + b_2x^2) f(x)$ [4]

Note: it is a convention in summation notation that if the sum extends to a range for which summands are not defined, then the undefined summands are taken to be zero. So if $a_1 = 1$, $a_2 = 2$ and $a_3 = 3$ are the only defined summands, then $\sum_{i=0}^4 a_i = 0 + 1 + 2 + 3 + 0 = 6$.

- (b) Verify that $\mathbb{Z}_7[x]$ satisfies the ring axiom R6:
if $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}_7[x]$ and $g(x) = \sum_{j=0}^m b_j x^j \in \mathbb{Z}_7[x]$, where $m, n \geq 0$ are integers, then $f \cdot g \in \mathbb{Z}_7[x]$. [4]
- (c) (i) Write down the units in $\mathbb{Z}_7[x]$. [2]
(ii) Find the unique monic polynomial that is an associate of 4 in $\mathbb{Z}_7[x]$. [2]
(iii) Find the unique monic polynomial that is an associate of $5x^2 + 3$ in $\mathbb{Z}_7[x]$. [2]

Question 9 – 11 marks

In this question, you will gain practice in testing the axioms for rings and fields, and help in understanding how to manipulate general algebraic expressions.

Let $R = (\mathbb{Z}, \oplus, \odot)$ denote the set of integers equipped with the operations $\oplus$ and $\odot$ defined as follows. For $a, b \in \mathbb{Z}$,

$$a \oplus b = a + b + 1,$$

$$a \odot b = ab + a + b.$$

- (a) Prove that $R = (\mathbb{Z}, \oplus, \odot)$ is a commutative ring. [5]
- (b) Is R an integral domain? Justify your answer. [3]
- (c) Is R a field? Justify your answer. [3]

Question 10 – 14 marks

This question asks you to use norms, irreducibles and primes to find a family of rings $\mathbb{Z}[\sqrt{-n}]$ that are not UFDs.

Let $n > 2$ be an even integer that is not divisible by 4.

- (a) Show that the norm $N(a + b\sqrt{-n}) = a^2 + nb^2$ is a multiplicative norm for $\mathbb{Z}[\sqrt{-n}]$. [2]
 - (b) Show that if u is a unit in $\mathbb{Z}[\sqrt{-n}]$, then $N(u) = 1$, and hence find all the units in $\mathbb{Z}[\sqrt{-n}]$. [3]
 - (c) Prove that the element 2 is irreducible in $\mathbb{Z}[\sqrt{-n}]$. [5]
 - (d) Show that 2 does not divide $\sqrt{-n}$. [1]
 - (e) By showing that 2 is not prime in $\mathbb{Z}[\sqrt{-n}]$, prove that $\mathbb{Z}[\sqrt{-n}]$ is not a UFD. [3]
-